REMARKS

The comments of the Applicant below are each preceded by related comments of the Examiner (in small, bold type).

2. Claims 1, 2, 6-10, 14-19, 21-22 and 41 rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al., (Porras), U.S. Patent No. 6,704,874 in view of Shostack et al. (Shostack), U.S. Patent No. 6,298,445.

As per claims 1 and 17:

Porras substantially teaches a method comprising:

detecting possible security problems at two or more client locations (3:16-4 1);

transmitting notice of the possible security problems from the two or more client locations across a network to a home location remotely located from the two or more locations (3.36-41);

determining at the home location an anomaly at one of the client locations based on an analysis of at least the possible security problems at the two or more client locations (5:63-6:33); and

transmitting notice of the anomaly in real time to the client locations (6:34-37).

Porras fails to teach performing the above steps in real time. However, Shostack discloses a real-time intrusion detection system that detects security problems, analyzes and alerts users (6:53-65).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to perform theses actions in real time in order to provide the most up to date security information and to remedy the problem as quickly as possible as recited in Shostack (2:31-47).

Claim 1

Porras does not disclose and would not have suggested notifying the client locations of the anomaly in real time, including "notifying the client locations to update collection of security data to include information about the anomaly," as recited in amended claim 1.

Porras does not disclose or suggest updating the collection of security data at client locations after an anomaly is determined at the home location, let alone notifying the client locations about the updating in real time.

Applicant disagrees with the Examiner's assertion that column 6, lines 34-37 of Porras discloses transmitting notice of the anomaly in real time to the client locations, as recited in claim 1. Porras discloses sending alerts from security and fault monitoring systems 22 to an alert manager 24, which generates a report based on the alerts and sends the report to a remote processing center 26 (col. 3, lines 34-30 and col. 6, lines 28-32). In column 6, lines 34-37,

Porras discloses that transport of the report occurs over an SSL for display and assessment by an end-user.

If the Examiner contends that the "end-user" of Porras corresponds to the "client location" of claim 1, then Porras does not disclose or suggest "transmitting notice of the possible security problems from the two or more client locations across a network to a home location remotely located from the two or more client locations," as recited in claim 1. In Porras, the alerts are sent from the security and fault monitoring systems 22 to the end-users (col. 4, lines 33-36). The end-users of Porras do not send alerts.

If the Examiner contends that the security and fault monitoring systems 22 or networks 12-14 of Porras correspond to the "client locations" of claim 1, then Porras does not disclose notifying the client locations in real time, as recited in claim 1. Porras does not disclose or suggest sending notices of anomalies to the security and fault monitoring systems 22 or networks 12-14.

What is lacking in Porras is also not disclosed or suggested in Shostack.

Claims 9 and 17

Claims 9 and 17 are patentable for at least similar reasons as those applied to claim 1.

As per claim 41 :

Porras discloses a method comprising:

detecting a possible security problem at a client location (3: 16-41);

transmitting notice of the possible security problems across a network to a home location remotely located from the client locations (3:36-41);

determining, at the home location, an anomaly at one of the locations based on the possible security problems by searching for particular information in the anomaly, the particular information including at least one of a network address previously noted as a security problem and a particular query or command associated with a known intrusion pattern or technique, in which detecting possible security problems at the two or more client locations (5:63-6:33, 5:28-44); and

transmitting notice of the anomaly in real time to the client locations (6:34-37).

Porras fails to teach performing the above steps in real time. However, Shostack discloses a real-time intrusion detection system that detects security problems, analyzes and alerts users (6:53-65).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to perform theses actions in real time in order to provide the most up to date security information and to remedy the problem as quickly as possible as recited in Shostack (2:31-47).

Claim 41

Porras does not disclose and would not have suggested determining an anomaly at one of the client locations based on the possible security problems by searching for particular information in the anomaly, the particular information including a particular query or command associated with a known intrusion pattern or technique, as recited in claim 41.

Porras discloses examining alert parameters that include a variable combination of attack type, timestamp, monitor ID, user ID, process ID, and IP / port addresses. Porras does not disclose or suggest searching for a particular query or command associated with a known intrusion pattern or technique.

What is lacking in Porras is also not disclosed or suggested in Shostack.

3. Claims 28, 30 and 32-34 rejected under 35 LI.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack), U.S. Patent No. 6,298,445 in view of Porras et al., (Porras), U.S. Patent No. 6,704,874.

As per claim 30:
Shostack substantially teaches a system comprising:

a server (9: 10):

for each of the client terminals, a first client mechanism accessible by the client terminal to detect a possible security problem at the client terminal (6:43-46, wherein an intrusion is a possible security problem),

a second client mechanism accessible by the client terminal to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem), and

a third client mechanism accessible by the client terminal to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems (7:57-63; 9: 10-21, wherein the client receives the software enhancement updates which function as updates from the server about security problems);

determining an anomaly continuously in real time (7: 15-1 6, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

a second server mechanism accessible by the server to transmit notice of the anomaly in real time over the network to the client terminals (7:57-63; 9: 10-2 1, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining an anomaly at one of the client terminals based on at least information received from the two or more client terminals regarding possible security problems. However, Porras discloses determining an anomaly based on alerts of possible security problems received from two or more clients (553-6:35).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to determine an anomaly based on possible security problems at two or more clients because this would allow detection of nominally different alerts may actually represent a single intrusion incident as taught by Porras (6:5- 12).

Claim 30

Shostack does not disclose and would not have suggested a second server mechanism to transmit notice of an anomaly in real time over a network to client terminals at which possible security problems are detected, the notice notifying the client terminals to update collection of security data to include information about the anomaly, as recited in amended claim 30.

Although Shostack discloses that a first application 48 distributes to each computer on a network 20 information about network status (col. 6, lines 58-59), Shostack does not disclose or suggest updating the collection of security data at client locations after an anomaly is determined at a home location.

What is lacking in Shostack is also not disclosed or suggested in Porras.

Claim 28

Claim 28 is patentable for at least similar reasons as those applied to claim 30.

4. Claims 40, 45, 48, 50 and 51 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack), U.S. Patent No. 6,298,445 in view of Porras et al., (Porras), U.S. Patent No. 6,704,874 as applied to claim 28 and further in view of Shipley (U.S. 6,119,236).

As per claim 40:

a server (9: 10);

for each of the client terminals,

a first client mechanism accessible by the client terminal to detect a possible security problem at the client terminal (6:43-46, wherein an intrusion is a possible security problem),

a second client mechanism accessible by the client terminal to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem), and

a third client mechanism accessible by the client terminal to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems (7:57-63; 9:lO-21, wherein the client receives the software enhancement updates which function as updates from the server about security problems);

determining an anomaly continuously in real time (7: 15-1 6, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

a second server mechanism accessible by the server to transmit notice of the anomaly in real time over the network to the client terminals (7:57-63; 9: 10-2 1, wherein the

software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining an anomaly at one of the client terminals based on at least information received from the two or more client terminals regarding possible security problems. However, Porras discloses determining an anomaly based on alerts of possible security problems received from two or more clients (5:63-6:35).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to determine an anomaly based on possible security problems at two or more clients because this would allow detection of nominally different alerts may actually represent a single intrusion incident as taught by Porras (6:5-12).

Shostack and Porras fail to teach the updates being applied to a firewall. However, Shipley discloses dynamically programming firewalls in real time to account for an anomaly (758-8:41).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Porras with the invention of Shipley because each uses firewalls in their own inventions individually and utilizing Shipley's real time dynamic programming of the firewalls would allow the firewalls to better protect their respective networks since it would constantly be modified to account for the newest threats (Shipley, 2:56-65).

As per claims 45 and 48:
Shipley further discloses a method further comprising storing and performing complex analysis of anomaly trends by using a complexity theory mechanism (5:58-6:3).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Porras with the invention of Shipley because each uses firewalls in their own inventions individually and utilizing Shipley's real time dynamic programming of the firewalls would allow the firewalls to better protect their respective networks since it would constantly be modified to account for the newest threats (Shipley, 2:56-65).

Claim 40

Shipley does not disclose and would not have suggested at least one of collecting information on users by using a human immune mechanism and checking and storing names and addresses associated with security problems by using a fingerprinting mechanism, as recited in amended claim 40.

Shipley discloses a "look for known code" operation that examines data for known bits of code, packet addresses, or other data characteristics in real time (col. 5, line 57 to col. 6, line 3). However, Shipley does not disclose or suggest collecting information on users by using a human immune mechanism, or checking and storing names and addresses associated with security problems by using a fingerprinting mechanism, as recited in claim 40.

7. Claims 42 and 52 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) and further in view of Moran, U.S. Patent No. 6,826,697.

As per claim 42:
Shostack discloses a method comprising:
detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);
transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);
transmitting notice of the anomaly in real time to the client location (7:57-63; 9: 10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location, including searching for an unexpected login. However, Lyle discloses a method wherein the event, which consists of an attack, is compared to other events that have occurred (7:50-8:ll).

Shostack and Lyle fail to teach a method in which determining the anomaly comprises searching for an unexpected login. However, Moran discloses a method wherein failed login attempts are logged (1 9:41-20: 18). A failed login attempt is an unexpected login since it is not a correct login. The login is not expecting for the login information to be wrong, therefore a failed login qualifies as an unexpected login by an unexpected user.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with Moran because in order to make a system less vulnerable to attack as stated in Shostack (2: 18-28), the ability to detect further types of attacks such as forward and backward time steps in a log file or an overflow buffer attack as stated in Moran (4: 1-37) would increase the security against attacks as a whole.

Claim 42

Moran does not disclose and would not have suggested searching for a "successful but unexpected login," as recited in claim 42. The Examiner asserts that a "failed login" qualifies an "unexpected login". The Applicant disagrees. Claim 42 recites searching for a "successful but unexpected login." What Moran discloses is logging failed login attempts. A "failed" login attempt is an attempt to login that failed. A "failed" login attempt is not a "successful" but unexpected login. According to the Examiner's logic, someone who "fails a test" would qualify as someone who "successfully but unexpectedly passes a test."

The Applicant also disagrees with Examiner's assertion that "the login is not expecting for the login information to be wrong." The login expects the login information to be wrong

when the login information is provided by unauthorized users. This is the purpose of the login process – authorized users are expected to provide correct login information, non-authorized users are expected provide incorrect login information, and therefore authorized users are able to login while unauthorized users cannot.

All of the dependent claims are patentable for at least the same reasons as those applied to the claims on which they depend.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner. Any circumstance in which the applicant has made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims. Any circumstance in which the applicant has amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: July 30, 2007

/Rex I. Huang/
Rex I. Huang
Reg. No. 57,661

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906